

## HIPAA Business Associate Agreement

This Business Associate Agreement (“Agreement”) is entered into this \_\_\_\_ day of \_\_\_\_\_, 2024 between \_\_\_\_\_ (“Covered Entity”) and \_\_\_\_\_ (“Business Associate”).

### RECITALS

I. Business Associate is a \_\_\_\_\_ company with a principal place of business at: \_\_\_\_\_

II. Covered Entity defined herein under the Health Insurance Portability and Accountability Act (“HIPAA”) and the Health In Technology for Economic and Clinical Health Act (“HIPAA/HITECH”) is required to enter into this Agreement to obtain satisfactory assurances that Business Associate, under HIPAA/HITECH, will appropriately safeguard all Protected Health Information (“PHI”) as defined herein, disclosed, created or received or with which Business Associate may come in contact with or have access to, by Business Associate on behalf of, Covered Entity to meet the requirements of privacy standards set forth in Section 164.504 (“Privacy Rule”), and 45 CFR 164.314 (“Security Rule”) and pursuant to the American Recovery and Reinvestment Act of 2009 (42 USC Section 17931 (a) et. Seq.) (“ARRA”).

III. Covered Entity desires to engage Business Associate to perform certain functions for, or on behalf of, Covered Entity involving the disclosure of PHI by Covered Entity to Business Associate, or the creation or use of PHI by Business Associate on behalf of Covered Entity, and Business Associate desires to perform such functions.

In consideration of the mutual promises below and the exchange of information pursuant to this agreement and in order to comply with all legal requirements for the protection of this information, the parties therefore agree as follows:

#### A. Definitions

##### Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

##### Specific definitions:

(a) Business Associate. “Business Associate” shall generally have the same meaning as the term “Business Associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean as named Business Associate listed above.

(b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “Covered Entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean “\_\_\_\_\_.”

(c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

## **B. Obligations and Activities of Business Associate**

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

(d) Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI in violation of this BAA. Business Associate agrees to reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this Agreement and/or any Security Incident or Breach. Business Associate shall also reasonably cooperate and coordinate with Covered Entity in the preparation of any reports or notices to the Individual, a regulatory body or any third party required to be made under HIP AA or any other Federal or State laws, rules or regulations, provided that any such reports or notices shall be subject to the prior written approval of Covered Entity. Business Associate shall keep Covered Entity fully apprised of all mitigation efforts of the Business Associate required under this Section.

(e) Reporting of Improper Access, Use or Disclosure. Business Associate shall promptly report to Covered Entity, in writing, any access, use or disclosure of PHI not permitted by the Agreement, this BAA, or applicable laws; and any security incident, as defined in the Security Rule, of which it becomes aware. Business Associate shall, following the discovery of any Breach of Unsecured PHI, notify Covered Entity in writing of such breach without unreasonable delay and in no case later than twenty-four (24) hours after discovery. The notice shall include the following information if known (or can be reasonably obtained) by Business Associate: (i) contact information for the individuals who were or who may have been impacted by the Breach (e.g., first and last name, mailing address, street address, phone number, email

address); (ii) a brief description of the circumstances of the Breach, including the date of the Breach and date of discovery (as defined in 42 U.S.C. Section 17932(c)); (iii) a description of the types of Unsecured PHI involved in the Breach (e.g., names, social security numbers, date of birth, addresses, account numbers of any type, disability codes, diagnostic and/or billing codes and similar information); (iv) a brief description of what Business Associate has done or is doing to investigate the Breach, mitigate harm to the individuals impacted by the Breach.

(f) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(g) Make available protected health information in a designated record set to the individual or the individual's designee as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524; The Business Associate will respond to a request for access that the Business Associate receives directly from the individual by forwarding within 5 working days, the individual's request to the Covered Entity to be fulfilled by the Covered Entity.

(h) The Business Associate will forward to Covered Entity any request for amendment(s) to protected health information in a designated record set to the Covered Entity pursuant to 45 CFR 164.526. within 5 working days.

(i) Maintain and make available the information required to provide an accounting of disclosures to the individual as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;

(j) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

(k) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

### **C. Permitted Uses and Disclosures by Business Associate**

(a) Business Associate may only use or disclose protected health information as necessary to perform the services set forth in Service Agreement. The Business Associate is not authorized to use protected health information to de-identify the information..

(b) Business Associate may use or disclose protected health information as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures.

(d) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.”]

(e) Business Associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(f) Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) Business Associate may provide data aggregation services relating to the health care operations of the Covered Entity.

**D. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

(a) Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of protected health information.

**E. Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

**F. Indemnification**

Indemnification. Each party will indemnify and hold harmless the other party to this Agreement from and against all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in conjunction with:

(a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this Agreement; and

(b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with the party’s performance under this agreement.

## **G. Term and Termination**

(a) Term. The Term of this Agreement shall commence on the date set forth above and end one year thereafter (the "Initial Term"). The Agreement shall renew automatically for successive one year period (each, a "Renewal Term") unless one party notifies the other party of its intent not to renew within thirty days prior to the end of the Initial Term or any Renewal Term. In addition, Covered Entity may terminate this Agreement for cause as authorized in paragraph (b) of this Section.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement.

(c) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining protected health information that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information;
4. Not use or disclose the protected health information retained by Business Associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

## H. Miscellaneous

(a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(d) Change in Law. In the event that there are subsequent changes or clarifications of statutes, regulations or rules relating to Agreement, Business Associate shall take all actions it reasonably deems are necessary to comply with such changes.

(e) Severability. In the event any provision of this Agreement is held to be unenforceable for any reason, the unenforceability thereof shall not affect the remainder of this Agreement, which shall remain in full force and effect and enforceable in accordance with its terms.

(f) Counterparts. This Agreement may be executed in counterparts, any of which is considered to be an original agreement.

[Signatures on Following Page]

IN WITNESS WHEREOF, each of the undersigned has caused this Amendment to be duly executed in its name and on its behalf effective as of date signed below.

**Covered Entity Name:**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Business Associate:**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_